

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION  
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international



(43) Date de la publication internationale  
3 mai 2001 (03.05.2001)

PCT

(10) Numéro de publication internationale  
**WO 01/31436 A1**

(51) Classification internationale des brevets<sup>7</sup>: **G06F 7/72**

Louis [FR/FR]; 3. rue Brown Séquard, F-75015 Paris (FR).

(21) Numéro de la demande internationale:

PCT/FR00/02978

(74) Mandataire: **BULL S.A.**: Corlu, Bernard, PC58D20. 68, route de Versailles, F-78434 Louveciennes cedex (FR).

(22) Date de dépôt international:

26 octobre 2000 (26.10.2000)

(81) États désignés (*national*): JP, US.

(25) Langue de dépôt:

français

(26) Langue de publication:

français

(84) États désignés (*régional*): brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

(30) Données relatives à la priorité:

99/13507

28 octobre 1999 (28.10.1999) FR

Publiée:

— Avec rapport de recherche internationale.

(71) Déposant (*pour tous les États désignés sauf US*): **BULL CP8** [FR/FR]; 68, route de Versailles, Boîte postale 45, F-78430 Louveciennes (FR).

*En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.*

(72) Inventeur; et

(75) Inventeur/Déposant (*pour US seulement*): **GOUBIN,**

(54) Title: SECURITY METHOD FOR A CRYPTOGRAPHIC ELECTRONIC ASSEMBLY BASED ON MODULAR EXPONENTIATION AGAINST ANALYTICAL ATTACKS

(54) Titre: PROCEDE DE SECURISATION D'UN ENSEMBLE ELECTRONIQUE DE CRYPTOGRAPHIE A BASE D'EXPONENTIATION MODULAIRE CONTRE LES ATTAQUES PAR ANALYSE PHYSIQUE

(57) Abstract: The invention concerns a security method for an electronic assembly implementing a cryptographic computation process using a modular exponentiation of a quantity ( $x$ ), said modular exponentiation utilising a secret exponent ( $d$ ). The invention is characterised in that it consists in breaking down said secret exponent into a plurality of  $k$  unpredictable values ( $d_1, d_2, \dots, d_k$ ) whereof the sum is equal to said secret exponent.

(57) Abrégé: L'invention concerne un procédé de sécurisation d'un ensemble électronique mettant en oeuvre un processus de calcul cryptographique faisant intervenir une exponentiation modulaire d'une grandeur ( $x$ ), ladite exponentiation modulaire utilisant un exposant secret ( $d$ ), caractérisé en ce que l'on décompose ledit exposant secret en une pluralité de  $k$  valeurs imprévisibles ( $d_1, d_2, \dots, d_k$ ) dont la somme est égale audit exposant secret.

WO 01/31436 A1